

ОБЕДИНЕНО УЧИЛИЩЕ „НЕОФИТ РИЛСКИ” – ДЕРМАНЦИ

ЗАПОВЕД

№ 157/16-25.09.2023 г.

На основание чл. 259, ал. 1 от Закона за предучилищното и училищното образование и чл. 24, параграф 2 от Регламента (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. и във връзка с необходимостта от защитата на физическите лица при обработването на лични данни

I. УТВЪРЖДАВАМ:

1. Актуализирана Вътрешна политика за защита на личните данни.

II. НАРЕЖДАМ:

2. В срок до десет работни дни от издаването на настоящата заповед, утвърдената Политика за защита на личните данни с приложенията ѝ, да се доведе до знанието на всички служители в институцията за сведение и изпълнение, което се удостоверява лично с подпис.

3. За неизпълнение на разпоредбите на утвърдената Политика за защита на личните данни с приложенията ѝ, виновните лица носят дисциплинарна отговорност.

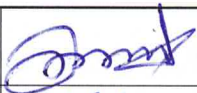
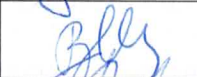
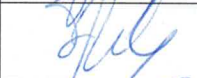
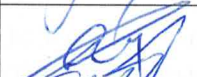
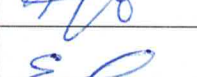
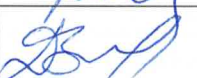
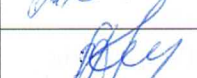
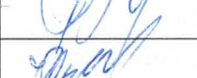
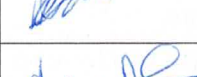
Директор: _____



ЗАПОЗНАТИ СЪС ЗАПОВЕДТА:

№ по ред	Име и фамилия	Заемана длъжност	Подпис на лицето	Дата на запознаване
1	Дияна Делчева Кордова	ЗДУД		25.09.2023г.
2	Гаврил Николов Трифонов	Педагог.съвет.		25.09.2023г
3	Богдана Василева Боданова	Психолог		25.09.2023г
4	Ани Лъчезарова Лазарова	ИКТ		25.09.2023г
5	Красимира Иванова Маринова	Уч.гимназ. етап		25.09.2023г
6	Татяна Антонова Маринова	Уч.гимназ. етап		25.09.2023г
7	Елена Георгиева Пандева	Уч.прог. етап		25.09.2023г
8	Радка Нейкова Иванова	Уч.теор и обуч.		25.09.2023г
9	Мария Георгиева Иванова	Уч. ГЦОУД 1-4кл		25.09.2023г
10	Маргарита Начева Калчева	Гл.учител прог.		25.09.2023г

Заповед за актуализиране на Политика за защита на личните данни

11	Пламен Георгиев Георгиев	Ст.учител прог.		25.09.2023г
12	Цветислава Стоянова Игнатова	Уч.прог.етап		25.09.2023г
13	Даниел Атанасов Симеонов	Уч.прог.етап		25.09.2023г
14	Емилия Пламенова Стойчева	Уч.прог.етап		25.09.2023г
15	Цветелина Ст.Петрова	Ст.уч.нач.етап		25.09.2023г
16	Виолета Иванова Тодорова	Ст.уч.нач.етап		25.09.2023г
17	Лора Петкова Иванова	Уч.нач.етап		25.09.2023г
18	Снежана Тонева Томова	Уч.нач.етап		25.09.2023г
19	Теодора Мирославова Кирилова	Уч.ГЦОУД 1-4кл.		25.09.2023г
20	Татяна Симеонова Христова	Уч.ГЦОУД 1-4кл		25.09.2023г
21	Николай Динков Граждански	Уч.ГЦОУД 1-4кл		25.09.2023г
22	Йорданка Георгиева Христова	Уч.ГЦОУД 1-4кл		25.09.2023г
23	Емил Йорданов Игнатов	Уч.ГЦОУД 5-7кл		25.09.2023г
24	Веселин Христов Николов	Уч.ГЦОУД 5-7кл		25.09.2023г
25	Калин Тотев Минчев	ЗАС		25.09.2023г
26	Венцислава Дакова Дилова	Домакин		25.09.2023г
27	Веселина Петрова Василева	Чистач		25.09.2023г
28	Галина Асенова Денчовска	Чистач		25.09.2023г
29	Теодора Цветанова Димитрова	Чистач		25.09.2023г
30	Трифон Йорданов Иванов	Огняр		25.09.2023г
31	Людмил Цвятков Лилов	Шофьор		25.09.2023г
32	Рахма Джамалова Алиева	Готвач		25.09.2023г
33	Нино Стефанов Йорданов	Обр.медиатор		25.09.2023г
34	Гана Самуилова Сутрузи	Обр.медиатор		25.09.2023г

ОБЕДИНЕНО УЧИЛИЩЕ „Неофит Рилски” - Дерманци

с. Дерманци
ул. „Христо Ботев” 16

www.ou-nrilski.com
e-mail: dermanci06@mail.bg

АКТУАЛИЗИРАМ
ДИРЕКТОР:



/Петя Кръстева/

ВЪТРЕШНА ПОЛИТИКА за мерките за защита на личните данни в Обединено училище „Неофит Рилски”

ВЪВЕДЕНИЕ

Ръководството на Обединено училище „Неофит Рилски” разбира, оценява и подкрепя всички усилия и мерки, насочени към осигуряване сигурността на личните данни и защитата на правата, свободите и интересите на физическите лица, чиито данни обработваме. С настоящата вътрешна политика ОБУ „Неофит Рилски” се ангажира да осигури съответствие със законодателството на ЕС и държавите-членки по отношение на обработването на личните данни и защитата на правата и свободите на физическите лица, чиито лични данни събира и обработва и прилага стриктно и в пълнота всички принципи за защита на личните данни, регламентирани в Общия регламент относно защитата на данните (ЕС) 2016/679 и законодателството на Европейския съюз и Република България.

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Обединено училище „Неофит Рилски” е юридическо лице със седалище с.Дерманци, общ. Луковит, обл. Ловеч, Република България с основен предмет на дейност образование и образователни услуги, наричано за краткост „Училището“.

(1) Информация за връзка с Училището:

Име: ОБУ „Неофит Рилски”
Адрес: ул. „Христо Ботев” 16
ЕИК: 000281864
телефон: 06979013
e-mail: dermanci06@mail.bg
уебсайт: www.ou-nrilski.com

(2) Информация за административен представител на Училището:

Име: Калин Тотев Минчев
Длъжност: завеждащ административна служба
телефон: 0897091701
e-mail: dermanci06@mail.bg

(3) Информация за длъжностно лице по ЗЗЛД

Име: Жана Караславова

Чл. 2. ОБУ „Неофит Рилски” е АДМИНИСТРАТОР на лични данни по смисъла на чл.3, ал.1 от Закона за защита на личните данни и чл.4 от Общия регламент относно защитата на данните (ЕС) 2016/679. На това основание Училището обработва лични данни във връзка със своята дейност и само определя целите и средствата за обработването им.

(1) Дани за представител на Училището, длъжностно лице по защита на личните данни, действащ под ръководството на администратора във връзка с изпълнение на служебни задължения относно Защитата на лични данни.

Име: Жана Караславова
телефон: 0887108760
e-mail: karaslavova_law@abv.bg

(2) Настоящите Вътрешни правила за обработване и защита на лични данни, определят реда, по който ОБУ „Неофит Рилски” обработва лични данни за целите на своята дейност, както и правилата за осигуряване защита на субектите на тези данни, във връзка с тяхното обработване.

(3) „Обработването” на лични данни по ал.1 включва всяка операция или съвкупност от операции извършвана с лични данни или набор от лични данни, в т.ч. събиране, записване, организиране, структуриране, съхраняване, адаптиране или променяне, извличане, консултиране, използване, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване, унищожаване или обработване по друг начин на лични данни.

(4) Вътрешните правила на ОБУ „Неофит Рилски” за обработване и защита на лични данни са изготвени на основание, в съответствие и в изпълнение на изискванията на Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (в частност на основание чл.24, пар.1 от Регламента), както и приложимото законодателство на Република България.

(5) Целта на настоящия документ е установяването на ясни правила при събиране, организиране, съхраняване и предоставяне на лични данни, обработвани от ОБУ „Неофит Рилски”, за да се гарантира неприкосновеността на личността и личния живот, като се защитят физическите лица при неправомерно обработване на свързаните с тях лични данни и се регламентират техните права и процедурите за упражняването им.

(6) Тези Правила уреждат:

1. Принципите, процедурите и механизмите за обработка на личните данни;
2. Основанията за обработване на личните данни;
3. Правата на субектите на лични данни;
4. Процедурите за администриране на искания от субектите на данни за упражняване на техните права;
5. Лицата, които обработват лични данни, и техните задължения;
6. Необходимите технически и организационни мерки за защита на личните данни от неправомерно обработване и в случай на инциденти, като случайно или незаконно унищожаване, загуба, неправомерен достъп, изменение или разпространение;
7. Процедурите и правилата, свързани с документиране и отчетност на обработването на лични данни;
8. Правилата за предаване на лични данни на трети лица в България и чужбина;
9. Процедурите по съхраняване и унищожаване, изтриване или заличаване на лични данни;
10. Процедурите за действия в случай на нарушения в сигурността;

(7) Тези Правила се прилагат спрямо всички лични данни, които обработваме, без значение от това какъв е техния източник и на какъв носител са съхранени.

(8) Правилата следва да се прилагат от и спрямо всички служители на институцията. Всички работници и служители следва да прочетат, да се запознаят с и да спазват съдържащите се в правилата политики при обработване на лични данни от името на институцията. Всяко нарушение на тези вътрешни правила е основание за налагане на дисциплинарни санкции спрямо работника или служителя, който го е допуснал.

Чл. 3. Като администратор на лични данни, при обработването на лични данни Училището спазва принципите за защита на личните данни, предвидени в Регламент (ЕС) 2016/679 и законодателството на Европейския съюз и Република България.

(1) Принципите за защита на личните данни са:

1. Законосъобразност, добросъвестност и прозрачност - обработване при наличие на законово основание, при полагане на дължимата грижа и при информиране на субекта на данни. ОБУ „Неофит Рилски” обработва лични данни само при наличие на законово основание, при полагане на дължимата грижа и при надлежно информиране на субекта на данни. С цел осигуряване на законосъобразност, преди обработването на лични данни задължително се идентифицира законово основание за обработване на данните. Законосъобразно е обработването на лични данни, което се основава на наличието на поне едно от следните условия:

- а. обработването е в изпълнение на законово задължение, което е предвидено в нормативен акт и се прилага спрямо Училището.
- б. обработването е необходимо за изпълнението на договор, по който субекта на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;
- в. обработването е необходимо, за да се защитят жизненоважни интереси на субекта на данните или на друго физическо лице;
- г. обработването е необходимо за изпълнение на задача от обществен интерес;
- д. обработването е необходимо за целите на легитимните интереси на ОБУ „Неофит Рилски” или на трета страна, освен когато пред тези интереси преимущество имат интересите или основните права и свободи на субекта на данни. В тези случаи целите на обработването се изписват изчерпателно в известието до субекта на данни.
- е. обработването се извършва въз основа на изричното съгласие на субекта на данни.

За да е законосъобразно, обработването на лични данни следва да е в съответствие и с цялото законодателство на ЕС и на Република България, а не само на законодателството, регламентиращо защитата на личните данни.

ОБУ „Неофит Рилски” няма да изисква съгласие от физически лица, чиито данни обработва, в случаите, когато за законосъобразното обработване на данните е налице друго годно основание. В случаите, когато изисква съгласие, институцията ще приема предоставянето му като годно основание за законосъобразно обработване на лични данни, когато са налице следните предпоставки:

1. Съгласието е изразено ясно, недвусмислено и конкретно, в разбираема и лесно достъпна форма, на ясен и прост език;
2. Съгласието е дадено чрез изявление или ясно утвърдителен акт (потвърждаващо действие), с който да се даде съгласие от страна на субекта на данни за обработване на свързани с него лични данни, например чрез писмена декларация, включително по електронен път;
3. Съгласието да е дадено информирано. За да бъде съгласието информирано, ОБУ „Неофит Рилски” за всеки конкретен случай ще предоставя на субекта на данни най-малко следната информация:
 - данни за администратора;
 - целта на всяка форма на обработване на данни;
 - вида лични данни, които ще се събират и обработват;
 - наличието на възможност за оттегляне на съгласието;

- дали данните ще се предават на трети лица и информация за свързаните с това рискове, ако не е налице решение за адекватно ниво на защита;
- какви са последиците при отказ да даване на съгласие.

Съгласието е дадено при наличие на действителен свободен избор на субекта да даде съгласието си, да откаже даването на съгласие или да оттегли вече даденото съгласие. Мълчаливото съгласие, предварително отметнатите полета във формуляр или декларация, и други, правят съгласието невалидно. Даденото съгласие се отнася за всички операции по обработване на данните.

ОБУ „Неофит Рилски” разбира и приема като "съгласие" само случаите, в които субектът на данните е бил напълно информиран за планираното обработване и е изразил своето съгласие без върху му да бъде упражняван натиск. Съгласието, получено при натиск или въз основа на подвеждаща информация, няма да се приема като валидно основание за обработване на лични данни. Образователната институция осигурява възможност за лесно оттегляне на даденото съгласие по всяко време, без да се засяга законосъобразността на обработването въз основа на съгласие преди оттеглянето му.

ОБУ „Неофит Рилски” обработва личните данни при съблюдаване на принципа за добросъвестност. Обработването е добросъвестно, когато не засяга неоправдано по неблагоприятен начин правата и свободите на физическите лица, субекти на данни, както и когато при обработването не се накърняват морала и добрите нрави.

Когато лични данни са предоставени на ОБУ „Неофит Рилски” от субекта на данни, без правно основание или в противоречие с принципите по чл. 5 от Регламента, институцията ги връща незабавно или ги изтрива, или унищожава в срок от един месец от узнаването.

ОБУ „Неофит Рилски” обработва лични данни при спазване на принципа за прозрачност, като предоставя детайлна и конкретна информация на субектите на данни.

Прилагането на принципа за прозрачност се гарантира от регламентираните в настоящите правила процедури за реализиране от субектите на данни на предоставените им право на информация и право на достъп.

Информацията по се предоставя чрез подходящи Информационни съобщения (Известия за поверителност) или Декларация за поверителност (Уведомление за поверително третиране на личните данни), по ред и начин, регламентирани в настоящите Правила.

2. Ограничение на целите – събиране на данни за конкретни, изрично указани илегалитимни цели и забрана за по-нататъшно обработване по начин, несъвместим с тези цели.

ОБУ „Неофит Рилски” събира лични данни на физически лица за конкретни, точно и ясно определени цели, и не може да ги обработва допълнително по начин, несъвместим с тези цели.

По-нататъшно обработване на личните данни за целите на архивирането в обществен интерес, за научни, исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели.

Целите, за които ОБУ „Неофит Рилски” обработва лични данни са:

1. управление на човешките ресурси, в т.ч. набиране и подбор на персонал, сключване, изпълнение и прекратяване на трудови и граждански договори с физически лица, изплащане на трудовите възнаграждения и изпълнение на свързаните с това задължения на ОБУ „Неофит Рилски” за удържане и плащане на здравни и социални осигуровки на служителите, на данъци, както и на други права и задължения на институцията в качеството ѝ на работодател по трудови договори или възложител по граждански договори;
2. изпълнение на основната си дейност като образователна институция – осъществяване на образователния процес и свързани с това други задължения;

(2) ОБУ „Неофит Рилски” не използва наличните лични данни за нови цели, различни и несъвместими с първоначалните цели, освен ако субекта на данни не предостави последващо съгласие за това.

3. Свеждане на данните до минимум – данните да са подходящи, свързани със и ограничени до необходимото във връзка с целите на обработването. Личните данни, които се събират и обработват следва да са подходящи, адекватни, релевантни, свързани с и ограничени до необходимото във връзка с целите на обработването.

ОБУ „Неофит Рилски” не събира информация от физическите лица – субекти на данни, която не е строго необходима за целта, за която тя е получена и се обработва. Длъжностното лице по защита на данните (ДЛЗД) се задължава да одитира ежегодно всички способности за събиране на данни, за да се гарантира, че събраните данни продължават да бъдат адекватни, релевантни и не са прекомерни с оглед на целите, за постигане на които се събират и обработват.

ОБУ „Неофит Рилски” осигурява навременното връщане или изтриване/унищожаване на всички лични данни, които вече не са необходими за конкретните цели.

4. Точност – поддържане в актуален вид и предприемане на всички разумни мерки за гарантиране на своевременно изтриване или коригиране на неточни данни, при отчитане на целите на обработването. ОБУ „Неофит Рилски” поддържа събраните лични данни точни, пълни и в актуален вид, във всеки един момент. Точността, пълнотата и актуалността на данните се проверява в момента на тяхното събиране, както и на регулярни интервали след това, но не по-малко веднъж годишно.

ОБУ „Неофит Рилски” предприема всички разумни мерки за унищожаването или корекцията на всички неточни или неактуални лични данни. За осигуряване и гарантиране точността и актуалността на данните, които ОБУ „Неофит Рилски” обработва като администратор, ще се прилагат следните мерки:

1. не се допуска съхраняване на данни, в случаите, когато има вероятност да не са точни.
2. лицата, които са натоварени с функции по събиране и обработване на лични данни са обучени в значението на събирането на точни данни и поддържането им в актуализиран вид.
3. въвежда се задължение на субекта на данни да декларира, че данните, които предава на ОБУ „Неофит Рилски” са точни и актуални. При изготвянето на формуляри и бланки, се включва изявление на субекта, че съдържащите се в документа данни са точни, верни и актуални към датата на подаване.
4. въвежда се изискване към всички субекти на данни да уведомяват ОБУ „Неофит Рилски” за всякакви промени в обстоятелствата, които изискват актуализиране на записите на лични данни.
5. прилагат се подходящи процедури и политики за поддържане на точност и актуалност на личните данни, като се отчита обемът на събраните данни, скоростта, с която може да се промени този обем и други относими фактори.
6. прилага се извършване на корекция на данни въз основа на искане за реализиране на правото на корекция;
7. надлежно и своевременно се информира всяка трета страна предоставила неточни или остарели лични данни, че информацията е неточна или остаряла, поради което не следва да се обработва и да се използва за вземане на решения относно лицата;
8. надлежно и своевременно се информират съответните получатели на лични данни, когато това е приложимо, и се препраща всяка корекция на лични данни, когато това е приложимо и необходимо.

5. Ограничение на съхранението – данните да се обработват за период с минимална продължителност съгласно целите. Съхраняване за по-дълги срокове е допустимо за

целите на архивирането в обществен интерес, за научни или исторически изследвания или статистически цели, но при условие, че са приложени подходящи технически и организационни мерки. ОБУ „Неофит Рилски” обработва лични данни само за период с конкретно определена продължителност съгласно целите, за които данните се обработват. Образователната институция не съхранява данните във формат, който да позволява идентифициране на субекта на данни за по-дълго време от необходимото за целите, за които данните са събрани. Съхраняване за по-дълги срокове е допустимо единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или статистически цели, но при условие, че са приложени подходящи технически и организационни мерки. С настоящите правила, ОБУ „Неофит Рилски” въвежда правила и политики относно съхранението на лични данни, които да осигурят и гарантират изтриване/унищожаване на данните, за които вече не съществува легитимна цел за обработване, освен в закон не е предвидено задължение за запазване и съхраняване на данните за определен минимален срок. Когато личните данни се запазват след датата на обработването, те ще бъдат съхранявани по подходящ начин, позволяващ да се защити самоличността на субекта на данните в случай на нарушение на данните.

6. Цялостност и поверителност – обработване по начин, който гарантира подходящо ниво на сигурност на личните данни, като се прилагат подходящи технически или организационни мерки. ОБУ „Неофит Рилски” обработва личните данни по начин, който гарантира подходящо ниво на сигурност, като се прилагат съответните технически и организационни мерки за това.

Изискването за цялостност се постига чрез такова обработване и съхраняване на данните, че същите да не могат да бъдат променени/подменени по неоторизиран начин в процеса на тяхното обработване, както и да не се дава възможност за изменение и за неразрешени манипулации на функциите по обработване на данните.

Изискването за поверителност (конфиденциалност) се постига чрез предприемане на мерки за неразкриване на личните данни на неоторизирани лица в процеса на тяхното обработване.

Изискването за наличност се постига чрез осигуряване на непрекъсната възможност за обработване на личните данни от оторизираните за това лица и за изпълнение на функциите на системата за обработване или бързото им възстановяване.

Образователната институция ще следва всички процедури и технологични мерки, които се въвеждат с настоящите Вътрешни правила или други нарочни процедури или инструкции, с цел опазване сигурността на личните данни от момента на тяхното събиране до момента на тяхното унищожаване.

7. Отчетност – администраторът носи отговорност и трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

Принципът за отчетност цели да гарантира, че обработването на личните данни се осъществява по осъзнат, прозрачен, надлежно документиран и следователно, лесно проследим и доказуем начин. С настоящите правила, ОБУ „Неофит Рилски” обезпечава прилагането на разпоредбите на ОРЗД, които насърчават отчетността и управляемостта и допълват изискванията за прозрачност при обработването на лични данни.

Институцията е отговорна за спазването на принципите за защита на личните данни и ги прилага по начин, който осигурява по всяко време възможност за доказване на тяхното спазване.

Възможността за доказване спазването на принципите за защита на данните се обезпечава и чрез инвентаризация на цялата вътрешна документация и интегриране в нея на конкретни процедури и политики от настоящите правила, както и чрез инвентаризация и актуализиране на всички договори с външни за институцията партньори, доставчици и други трети лица. Възможността за доказване спазването на принципите се реализира и

чрез преглед и актуализация на правното основание за предаване (трансфер) на данни към външни получатели, когато и ако това е приложимо.

II. ЦЕЛ НА ДОКУМЕНТА

Чл. 4. Настоящата Вътрешна Политика урежда условията и реда на събиране, обработване, контрол при обработването, водене на регистри, и защитата на лични данни на преподавателите, служителите, обучаемите (ученици), родителите, посетителите, доставчиците, както и на всички други групи физически лица, с които Училището влиза в отношения при осъществяването на правомощията и дейността си. Тя има за цел да гарантира, че се изпълняват всички относими закони свързани със защитата на личните данни.

III. ОБХВАТ

Чл. 5. Вътрешната Политика за защита на лични данни предоставя информация за целите на обработване на личните данни, категориите обработвани лични данни, получателите или категориите получатели, на които могат да бъдат разкрити данните, основанието за обработка на данни, задълженията на всички лица обработващи лични данни под ръководството на Училището или Обработващия лични данни, информация за правото на достъп и коригиране на събраните данни съгласно изискванията на Регламент 2016/679. Обхватът на настоящия документ е съобразен с изискванията в чл. 13 и чл. 14 от Регламент 2016/679.

Чл. 6. Съдържанието на документа е адресирано до преподавателите, служителите, обучаемите (ученици), родителите, посетителите, доставчиците, както и на всички други физически лица, свързани с осъществяването на нормалната дейност на училището, влизащи в обхвата на събраните лични данни.

IV. ИЗПОЛЗВАНИ ТЕРМИНИ И ДЕФИНИЦИИ

Чл. 7. По смисъла на настоящата Вътрешна Политика са използвани термини със следното значение:

ОРЗД (Общ регламент за защита на данните) или „Регламент(а)” - Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните);

• ЗЗЛД – Закон за защита на личните данни;

• КЗЛД – Комисия за защита на личните данни;

(1) „Лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;

1.1. „специални категории лични данни“ са лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице;

(2) „Обработване на лични данни“ означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или

промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбинирание, ограничаване, изтриване или унищожаване;

(3) **„Регистър с лични данни“** означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип;

(4) **„Администратор“** означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка;

(5) **„Обработващ лични данни“** означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

(6) **„Оператор на лични данни“** е всяко лице, което по указание и под ръководството на администратора има достъп до лични данни и упражнява ограничени функции по тяхната обработка съобразно нормативните актове, регламентиращи дейността на гимназията.

(7) **„Поверителност“** е изискване за неразкриване на личните данни на неоторизирани лица в процеса на тяхното обработване.

(8) **„Предоставяне на лични данни“** са действия по цялостно или частично пренасяне на лични данни от един администратор към друг или към трето лице на територията на страната или извън нея.

(9) **„Регистър на лични данни“** е всяка структурирана съвкупност от лични данни, достъпна по определени критерии, централизирана, децентрализирана или разпределена на функционален или географски принцип.

(10) **„Субект на данни“** – физическо лице, чиито лични данни са обект на обработване и което е идентифицирано или може да бъде идентифицирано чрез обработваните лични данни;

(11) **„Съгласие на субекта на данните“** - всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени;

(12) **„Длъжностно лице по защита на данните“** или ДЛЗД – физическо лице, юридическо лице или организация, определени съгласно изискванията на чл. 37 и сл. от ОРЗД;

(13) **„Лице с достъп до лични данни“** - всяко лице, действащо под ръководството на администратора или на обработващия, което има достъп до обработваните лични данни. Лицето може обработва данните само по указание на администратора/обработващия, освен ако в закон е предвидено друго;

(14) **„Регистър с лични данни“** - всеки структуриран набор от лични данни, независимо от неговия вид и носител, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип;

(15) **„Носител на лични данни“** - физически обект, на който могат да се запишат данни или могат да се възстановят от същия.

(16) **„Известия по защита на данните“** – отделни известия, съдържащи информация, предоставяна на субектите на данни в момента, в който институцията събира информация за тях. Тези известия могат да бъдат както общи, така и конкретно отнесени към обработването на лични данни със специфична цел.

(17) **„Получател“** - физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не.

Публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за „получатели“. Обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването;

(18) „Основно място на установяване“ – седалището на администратора в ЕС ще бъде мястото, в което той взема основните решения за целта и средствата на своите дейности по обработване на данни. По отношение на обработващия лични данни основното му място на установяване в ЕС ще бъде неговият административен център. Ако администраторът е със седалище извън ЕС, той трябва да назначи свой представител в юрисдикцията, в която администраторът работи, за да действа от името на администратора и да се занимава с надзорните органи.

(19) „Трета страна“ – всяко физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни;

(20) „Профилиране“ - всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение;

(21) „Автоматизирано вземане на решения“ - когато дадено решение е взето изцяло на базата на автоматизирано обработване (включително профилиране), което води до правни последици или засяга значително физическото лице.

(22) „Псевдонимизиране“ – заместването на информация, която директно или индиректно идентифицира физическо лице, с един или повече идентификатори („псевдоними“), така че лицето да не може да бъде идентифицирано без достъп до допълнителната информация, която следва да се съхранява отделно и да е поверителна.

(23) „Оценка на въздействието“ - механизми и мерки, използвани за идентифициране на риска, свързан с обработката на данните. Оценката на въздействието следва да бъде извършена за всички ключови системи или програми, свързани с обработването на лични данни.

V. ОСНОВАНИЕ ЗА ОБРАБОТКА

Чл. 8. В ОБУ „Неофит Рилски“ личните данни се събират за конкретни, точно определени от закона цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели.

Чл. 9. Обработването е законосъобразно, само ако и доколкото е приложимо поне едно от следните условия:

- (1) съгласие на субекта на данни (приложимо);
- (2) обработването е свързано и необходимо за изпълнението на договор (приложимо);
- (3) обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора (приложимо);
- (4) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;
- (5) обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора (приложимо);
- (6) обработването е необходимо за целите на легитимните интереси на администратора или на трета страна

VI. ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл. 10. Като администратор на лични данни ОБУ „Неофит Рилски” обработва лични данни чрез съвкупност от действия, които могат да се извършат по отношение на личните данни с автоматични или неавтоматични средства, като записване, събиране, организиране, съхраняване, употреба за посочените цели, предаване, заличаване, унищожаване.

Чл. 11. Обработването на лични данни се състои и в осигуряване на достъп до определена информация само за лица, чиито служебни задължения или конкретно възложени задачи налагат такъв достъп.

Чл. 10. ОБУ „Неофит Рилски” като администратор на лични данни, обработва определени категории лични данни, необходими за осъществяването на правомощията и дейността си.

Чл. 12. ОБУ „Неофит Рилски” събира и обработва лични данни, необходими за осъществяване на своите права и задължения като работодател и образователна институция, при съблюдаване изискванията на приложимото законодателство.

(2) Личните данни, обработвани от институцията като администратор на данни се отнасят до следните категории субекти на данни:

1. кандидати за работа;
2. работници / служители и изпълнители по граждански договори;
3. деца, ученици и родители;
4. други категории субекти, когато възникнат предпоставки за обработване на техни лични данни.

Чл.13. (1) Относно лицата, кандидатстващи за работа в институцията се събират следните лични данни:

1. Идентификация:

- ☐ трите имена;
- ☐ адрес за кореспонденция;
- ☐ телефон;
- ☐ електронен адрес;

2. Данни, свързани с образование, трудов опит, професионална и лична квалификация и умения;

3. В случаите, когато това е свързано с изискване за заемане на съответната длъжност, институцията изисква предоставянето на данни за здравословно състояние, медицински свидетелства, ТЕЛК решения, документи, удостоверяващи психическата пригодност.

4. Други данни, когато това е необходимо във връзка с длъжността, за която лицето кандидатства, напр. свидетелство за съдимост, данни от свидетелство за управление на МПС.

(2) Първоначалното събиране на лични данни от кандидатите за работа се извършва въз основа на депозирана от субекта на данни автобиография. При обработване на лични данни от автобиографии, ОБУ „Неофит Рилски” прилага следните правила:

1. Автобиографиите се представят от кандидатите за работа по един от следните начини:

- ☐ на хартиен носител - лично в деловодството на институцията или чрез пощенска пратка на адреса на институцията
- ☐ в електронен формат - чрез имейл на електронния адрес на институцията;

2. Данните от автобиографиите се обработват единствено във връзка с кандидатстването на физическото лице за работа в институцията и за оценка и подбор на кандидата;

3. Представените автобиографии и данните съдържащи се в тях не могат да се предоставят на трети лица;

4. Данните от автобиографиите се съхраняват до приключване на подбора за вакантното работно място, след което се унищожават по съответния ред;

(3) Образователната институция не съхранява данните на кандидатите за работа след приключване на процедурата по подбор.

(4) Когато в процедура по подбор, институцията е изисквала да се представят оригинали или нотариално заверени копия на документи, удостоверяващи физическа и психическа годност на кандидата, образованието, необходимата квалификационна степен и стаж за заеманата

длъжност, субектът на данните, който не е одобрен за назначаване, може да поиска в 30-дневен срок от окончателното приключване на процедурата по подбор да получи обратно представените документи. Институцията връща документите, по начина, по който са подадени.

Чл.14. (1) Относно лицата, заети по трудови или граждански правоотношения в институцията се събират следните лични данни:

1. Идентификация:

- ☐ трите имена;
- ☐ ЕГН/ЛНЧ;
- ☐ постоянен и настоящ адрес;
- ☐ телефонен номер;
- ☐ данни по лична карта или паспортни данни;

2. Образование и професионална квалификация: данни, свързани с образование, професионален опит, професионална и лична квалификация и умения, включително данни от свидетелство за управление на МПС;

3. Здравни данни: здравословно състояние, ТЕЛК решения, медицински свидетелства, болнични листове и всяка прилежаща към тях документация;

4. Данни за банкови сметки, които се обработват във връзка с изплащане на възнаграждения и обезщетения, в изпълнение на сключения трудов договор и нормативни разпоредби на трудовото и осигурителното законодателство;

5. Други данни: институцията изисква свидетелство за съдимост, само в случай, че за заемането на определена длъжност, в нормативен акт е предвидено изискване, свързано с липсата на осъдителни присъди или когато изрично се изисква представянето му съгласно нормативен акт.

(2) Лицето, натоварено с функции по обработване на личните данни на работниците /служителите може да копира документ за самоличност, свидетелство за управление на моторно превозно средство, документ за пребиваване на работник или служител, само ако това е изискване, предвидено в нормативен акт.

(3) Образователната институция обработва чувствителни данни (напр. данни за здравословното състояние или данни за съдебното минало) на работниците и служителите, само доколкото това е необходимо за изпълнение на специфичните ѝ права и задължения на работодател в областта на трудовото и осигурително законодателство.

Чл.15. (1) Относно деца, ученици и родители се събират лични данни, които са необходими за изпълнението на основната дейност и свързаните с това законови задължения на образователната институция, както следва:

1. Трите имена;
2. Единен граждански номер;
3. Гражданство;
4. Месторождение;
5. Данни от лична карта (на ученици над 14 години);
6. Адрес;
7. Електронен адрес (имейл);
8. Телефонен номер;
9. Данни за образованието на ученика;
10. Пол;
11. Данни за родители – имена, телефонен номер, адрес, месторабота и други;
12. Информация за присъствия и отсъствия;
13. Данни за успеха и оценяването на ученика;
14. Информация за полагане на изпити (НВО, ДЗИ, олимпиади, състезания, конкурси и други);
15. Информация за издаване на дипломи, удостоверения, свидетелства, ученически книжки и ученически лични карти;

16. Информация за здравно осигуряване (за ученици на възраст над 18 г.);
 17. Информация, необходима за предоставяне на стипендии;
 18. Информация във връзка със социално подпомагане;
- (2) ОБУ „Неофит Рилски” обработва и следните специални категории по-чувствителни данни за учениците:
1. Информация за здравословното състояние на учениците – вкл. здравно-профилактични карти, заболявания, наличие на трайни увреждания, имунизации, данни за личен лекар и т.н.;
 2. Информация за специални образователни потребности (когато е приложимо);
 3. Фото и видео-материали, вкл. снимки на учениците за техни досиета или документи.

VII. СРОК НА СЪХРАНЕНИЕ НА ЛИЧНИТЕ ДАННИ

Чл. 16. Личните данни се събират и съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на правомощия, правни задължения на Училището и/или нормалното му функциониране.

(1) Постъпилите искания за достъп до лични данни ще бъдат запазвани за не повече от 1 година от датата на подаването им. В края на разрешените срок исканията ще бъдат трайно и необратимо унищожавани.

Чл. 17. След постигане целта на обработване на личните данни или преди прехвърлянето на контрола върху обработването личните данни, съдържащи се в поддържаните от Училището регистри, следва да бъдат унищожени или прехвърлени на друг администратор на лични данни съобразно изискванията на Закона за защита на личните данни (чл. 25). При промени в структурата на училището, налагащи прехвърляне на регистрите за лични данни на друг администратор на лични данни, предаването на регистъра се извършва след разрешение на Комисията за защита на лични данни.

Чл. 18. В случаите, в които се налага унищожаване на носител на лични данни, Училището прилага необходимите действия за заличаването на личните данни по начин, изключващ възстановяване данните и злоупотреба с тях, като:

- (1) Личните данни, съхранявани на електронен носител и сървъри, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите;
- (2) Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване.
- (3) Унищожаване се осъществява от служители, упълномощени за тази дейност и след уведомяване на Длъжностното лице по защита на данните, ако има назначено такова.
- (4) За извършеното унищожаване на лични данни и носители на лични данни се съставя Протокол за унищожаване на лични данни, подписан от служителите по ал. 3, съгласно образец.

Чл. 19. Документите и преписките, по които работата е приключила, се архивират.

(1) Трайното съхраняване за нуждите на архивирането на документи, съдържащи лични данни, се извършва на хартиен носител в помещения, определени за целта, за срокове, съобразени с действащото законодателство. Помещенията задължително се заключват.

(2) Документите на електронен носител се съхраняват на компютърни системи и/или външни носители на информация. Архивните копия се съхраняват на различно местоположение от мястото на информационната система, обработваща данните. Достъп до архивираните документи, съдържащи лични данни, имат единствено оторизираните лица и администраторът съобразно възложените им правомощия.

VIII. ПОЛУЧАТЕЛИ, НА КОИТО СЕ ПРЕДОСТАВЯ ДОСТЪП ДО ЛИЧНИТЕ ДАННИ

Чл. 20. Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на искане за достъп на информация, и след тяхното легитимиране.

(1) Предоставяне на достъп до лични данни за съответното лице, Училището осигурява в 30-дневен срок от подаване на искането.

(2) Информацията може да бъде предоставена под формата на:

1. устна справка;
 2. писмена справка;
 3. преглед на данните от самото лице;
 4. предоставяне на исканата информация на технически и/или електронен носител.
- (3) Всеки трансфер на данни, включително използването на облачни услуги, извън ЕИП следва да бъде предварително съгласуван със СЗД/ДЛЗД с оглед изискването в ОРЗД за предприемането на определени мерки.

Чл. 21. Администраторът възлага обработването на личните данни на негови служители. Обработването се възлага на повече от един служител, съобразно спецификата на изпълняваните от тях служебни функции и с цел разграничаване на конкретните им задължения.

Чл. 22. Всеки правен субект, който обработва лични данни по възлагане и от името на администратора, е Обработващ лични данни.

(1) ОБУ „Неофит Рилски” възлага достъп и обработка на лични данни на външен Обработващ лични данни, като взаимоотношенията по между им се уреждат със сключен Договор за обработване на лични данни.

Чл. 23. Обработващият лични данни е юридическо лице, което действа само и единствено от името на Училището, в качеството на администратор.

(1) Данни за Обработващия лични данни от видеонаблюдение

Име: Василев Секюрити ЕООД

Адресна регистрация: гр. Луковит, ул. “Златна Панега” 20

ЕИК: 201394219

телефон: 0879 00 22 56

e-mail: vasilevsecurityeood@gmail.com

уебсайт: vasilev-security.com

Чл. 24. Училището не предвижда и не предоставя достъп до личните данни, които обработва на трети лица, независимо физически или юридически, различни от служителите на администратора или Обработващия лични данни, освен ако това не му се вмени от дадено законодателство.

Чл. 25. Училището ще предостави достъп до личните данни на органи имащи законово основание за обработването на лични данни (напр. съд, прокуратура, НАП, НОИ, Министерство на вътрешните работи, контролни органи, органи на местното самоуправление и т.н.), при отправено искане по съответния законов ред.

Чл. 26. Училището не предвижда и няма намерение да предоставя информация за личните данни в други държави, държави членки на Европейския съюз или държави извън Европейския съюз, освен ако това не му бъде наложено по законов ред.

IX. ПРАВА НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ

Чл. 27. Субектът на данни има право да получи от ОБУ „Неофит Рилски” потвърждение дали се обработват лични данни, свързани с него и ако това е така, да изиска от Училището информацията, съдържаща се в настоящата Вътрешна Политика и следното:

(1) Право на достъп до личните данни, отнасящи се до субекта; Правото на достъп се осъществява с писмено Искане за достъп.

- (2) Право на коригиране: субектът на данни има право да поиска от администратора да коригира без ненужно забавяне неточните лични данни, свързани с него.
- (3) Право на изтриване: Субектът на данни има правото да поиска от администратора изтриване на свързаните с него лични данни без ненужно забавяне, а администраторът има задължението да изтрие без ненужно забавяне личните данни, когато е приложимо и не възпрепятства спазването на правно задължение от страна на Училището.
- (4) Право на ограничаване на обработването: Субектът на данните има право да изиска от администратора ограничаване на обработването, когато се прилага едно от следното: точността на личните данни се оспорва от субекта на данните, за срок, който позволява на администратора да провери точността на личните данни; обработването е неправомерно, но субектът на данните не желае личните данни да бъдат изтрети; администраторът не се нуждае повече от личните данни за целите на обработването, но субектът на данните ги изисква за установяването, упражняването или защитата на правни претенции;
- (5) Право на преносимост на данните: Субектът на данните има право да получи личните данни, които го засягат и които той е предоставил на администратор, в структуриран, широко използван формат и пригоден за машинно четене ако е възможно.
- (6) Право на субекта на лични данни да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране. Училището не използва такива методи.
- (7) Право на възражение срещу обработването на лични данни: Субектът на данните има право, по всяко време и на основания, свързани с неговата конкретна ситуация, на възражение срещу обработване на лични данни, отнасящи се до него, което се основава на чл. 6, параграф 1, буква д) или буква е) от Регламент (ЕС) 2016/679. Администраторът прекратява обработването на личните данни, освен ако не докаже, че съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции.

Чл. 28. При неправомерно поискани допълнителни копия на лични данни, от субекта на данни, а както следва повече от два пъти за един и същ казус, АДМИНИСТРАТОРЪТ има право да изиска парична такса за обработване и предоставяне на данните.

Чл. 29. Задължение на Училището е да предостави достъп до лични данни на субекта, за които се отнасят в разумен срок от датата на подаване на искане за достъп, но най-късно в срок до един месец.

Чл. 30. Право на жалба

(1) Субектите на лични данни имат право да подадат жалба до надзорен орган, ако считат, че обработването на лични данни, отнасящи се до тях, нарушава приложимото законодателство по защита на личните данни. Надзорният орган в Република България е Комисията за защита на личните данни, с адрес: гр. София 1592, бул. „Проф. Цветан Лазаров” № 2, www.cpdp.bg, kzld@cpdp.bg, телефон на Център за информация и контакти – +359 (2) 91 53 518. Всички субекти на лични данни, учители, служители, ученици, родители и посетители имат право да упражнят правата си на място в Училището, в офиса на заместник директора по телефона или на електронен адрес, посочен в информацията за администратора.

Х. ЛИЦА, ОТГОВАРЯЩИ ЗА СЪБИРАНЕТО, ОБРАБОТВАНЕТО И СЪХРАНЕНИЕТО НА ЛИЧНИ ДАННИ И/ЛИ ИМАЩИ ДОСТЪП ДО ДАННИТЕ

Лица, управляващи процесите по обработване на лични данни

Чл.31. (1) Като администратор на лични данни, ОБУ „Неофит Рилски” се представлява от директора на образователната институция.

(2) Ръководството на институцията е отговорно за разработване и насърчаване използването на добри практики в сферата на защитата на личните данни.

Чл.32. (1) Директорът на ОБУ „Неофит Рилски” определя с писмен акт Длъжностно лице по защита на данните (ДЛЗД).

(2) За ДЛЗД може да бъде определено физическо или юридическо лице, което притежава познания в областта на защитата на данните - законодателство и практическо приложение.

(3) Определеното Длъжностно лице по защита на данните подпомага директора и останалите служители при реализиране на дейностите по обработване на данните и тяхната защита.

Чл.33. (1) Длъжностното лице по защита на данните има следните правомощия и задължения:

1. информира и съветва директора и служителите, които извършват обработване на лични данни, за техните задължения по силата на ОРЗД и на други разпоредби за защитата на данни на равнище Съюз или държава членка;

2. наблюдава спазването ОРЗД и на други разпоредби за защитата на данни на равнище Съюз или държава членка, както и разпоредбите на настоящите Правила, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване, и съответните одити;

3. сътрудничи си с надзорния орган, когато е изрично оправомощен за това от директора;

4. действа като точка за контакт за надзорния орган по въпроси, свързани с обработването и по целесъобразност се консултира по всякакви други въпроси;

5. следи за спазване на организационната процедура за обработване на личните данни, включваща време, място и ред при обработване, чрез регистрация на всички извършени действия с регистрите;

6. определя ред за съхраняване и унищожаване на информационни носители;

7. определя ред при задаване, използване и промяна на пароли, както и действията в случай на узнаване на парола и/или криптографски ключ;

8. определя правила за провеждане на редовна профилактика на компютърните и комуникационните средства, включваща и проверка за вируси, за нелегално инсталиран софтуер, на целостта на базата данни, както и архивиране на данни, актуализиране на системната информация и др.;

9. провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване;

10. изпълнява всички задължения по докладване и управление на нарушения на сигурността на данните;

11. унищожава данните от хартиените и техническите носители съгласно закона и сроковете, установени в тези Правила;

12. води регистър на дейностите по обработване на лични данни в ОБУ „Неофит Рилски”

(2) ДЛЗД е задължен да спазва секретността или поверителността на изпълняваните от него задачи в съответствие с правото на Съюза или правото на държава членка.

(3) ДЛЗД може да изпълнява и други задачи и задължения.

(4) При изпълнение на възложените по предходната алинея функции и правомощия, ДЛЗД действа като независим подпомагащ вътрешен орган и се отчита пряко пред Директора на институцията.

(5) Всички служители са длъжни да оказват съдействие на ДЛЗД при изпълнение на функциите му.

Лица, извършващи дейности по обработване на лични данни и/или имащи достъп до лични данни

Чл.34. (1) Достъп до личните данни, обработвани и съхранявани от ОБУ „Неофит Рилски” имат само служителите, на които такъв достъп е разрешен и необходим за изпълнение на служебните им задължения, както и за изпълнение на бизнес цели, при стриктно спазване на принципа „Необходимост да знае”.

(2) Оторизирането за достъп или извършване на дейности по събиране, обработване, съхранение и защита на личните данни се осъществява с нарочна заповед на директора или

чрез формулираните в длъжностната характеристика конкретни трудови функции и задължения.

(3) Възможността за достъп до личните данни на други служители на институцията се ограничава до случаите, когато на тях е предоставен такъв с изрично разрешение, в което се посочват личните данни и целите, за които се предоставя достъпът, както и времето, за което той се предоставя.

Чл.35. (1) Служителите на ОБУ „Неофит Рилски” са длъжни:

1. да обработват лични данни законосъобразно и добросъвестно;
2. да използват личните данни, до които имат достъп, съобразно целите, за които се събират, и да не ги обработват допълнително по начин, несъвместим с тези цели;
3. да актуализират при необходимост регистрите на личните данни;
4. да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
5. да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват;
6. да подпишат Декларация-Приложение №1 (за служители обработващи данни).

(2) Задълженията по предходната алинея се прилагат за всички длъжности в институцията, свързани с обработването на лични данни и/или имащи достъп до данните.

Чл.36. Работниците и служителите нямат право да разпространяват информация за личните данни, станали им известни при и по повод изпълнение на служебните им задължения.

Чл.37. (1) Всяко нарушение на правилата и ограниченията за достъп до личните данни от персонала може да бъде основание за налагане на дисциплинарни санкции по отношение на съответните работници и служители.

(2) Ако в резултат на действията на съответен служител по обработване на лични данни са произтекли вреди за ОБУ „Неофит Рилски” или за трето лице, от служителя може да се потърси имуществена отговорност по реда на общото гражданско законодателство.

XI. ПРАВА И ЗАДЪЛЖЕНИЯ НА ЛИЦАТА ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

Чл. 38. Право на достъп до лични данни имат държавните органи, съобразно възложените им от закона правомощия и оторизираните работници и служители на Училището, както и Обработващият лични данни и неговите служители, на които администраторът е възложил обработването на данни.

Чл. 39. Оторизирането на работници и служители се извършва на база длъжностна характеристика и/или чрез изрично ПЪЛНОМОЩНО от Директора на Училището.

Чл. 40. Длъжностните лица и служителите нямат право да разпространяват информация за личните данни, станали им известни при и по повод изпълнение на служебните им задължения.

(1) Нарушаването на поверителността на личните данни е и нарушение на законодателството за защита на данните и може да доведе до наказателен или граждански иск срещу Училището. Следователно всички обработващи лични данни в Училището трябва да се придържат към политиката за защита на личните данни и политиките, които допринасят за нейното изпълнение.

Чл. 41. При регистриране на неправилен достъп до информационните масиви за лични данни, или при друг инцидент, нарушаващ сигурността на личните данни, служителят, констатирал това нарушение/инцидент, незабавно докладва за това на прекия си ръководител - администраторът на лични данни, който от своя страна е длъжен, своевременно да информира Длъжностното лице по защита на данните за инцидента.

Чл. 42. Уведомяването на Комисията за защита на личните данни (КЗЛД) за възникнал инцидент се извършва от АДМИНИСТРАТОРА, писмено, по електронен път или по друг

начин, който позволява да се установи извършването му и да се спази изискването за уведомяване на КЗЛД в срок от 72 часа от узнаването за инцидента.

(1) Процесът по докладване и управление на инциденти задължително включва регистрирането на инцидента, времето на установяването му, лицето, което го докладва, лицето, на което е бил докладван, последствията от него и мерките за отстраняването му.

Чл. 43. Лице по защита на личните данни е адв. Жана Караславова.

(1) Лицето по защита на личните данни има следните правомощия:

1. осигурява организацията по водене на регистрите, съгласно предвидените мерки за гарантиране на адекватна защита;
2. следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно, спецификата на водените регистри;
3. осъществява контрол по спазване на изискванията за защита на регистрите;
4. поддържа връзка с Комисията за защита на личните данни относно предприетите мерки и средства за защита на регистрите и подадените заявления за предоставяне на лични данни;
5. контролира спазването на правата на потребителите във връзка с регистрите и програмно-техническите ресурси за тяхната обработка;
6. специфицира техническите ресурси, прилагани за обработка на личните данни;
7. следи за спазване на организационната процедура за обработване на личните данни, включваща време, място и ред при обработване, чрез регистрацията на всички извършени действия с регистрите в компютърната среда;
8. определя ред за съхраняване и унищожаване на информационни носители;
9. провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване.
10. определя ред при задаване, използване и промяна на пароли, както и действията в случай на узнаване на парола

(2) Лицето по защита на личните данни може да делегира своите пълномощия изцяло и/или частично на други лица.

Чл. 44. Служителите на Училището са длъжни:

- (1) да обработват лични данни законосъобразно и добросъвестно;
- (2) да използват личните данни, до които имат достъп, съобразно целите, за които се събират, и да не ги обработват допълнително по начин, несъвместим с тези цели;
- (3) да актуализират регистрите на личните данни (при необходимост);
- (4) да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
- (5) да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват.
- (6) да не разгласяват лични данни, до които са получили достъп при и по повод изпълнение на задълженията си.

Чл. 45. Работниците и служители носят отговорност за спазването на разпоредбите на настоящата политика; за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на регистрите, съдържащи лични данни. Всяко нарушение на сигурността, правилата и ограниченията за обработка и достъп до личните данни от персонала ще бъде разгледано в съответствие с правила на Вътрешната политика и съответните дисциплинарни политики, може да бъде основание за налагане на дисциплинарни санкции по отношение на съответните работници и служители.

Чл. 46. Ако в резултат на действията на съответен служител по обработване на лични данни са произтекли вреди за Училището или за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство.

XII. МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 47. ОБУ „Неофит Рилски” организира и предприема мерки, за защита на личните данни от случайно или незаконно унищожаване, от неправомерен достъп, от изменение или разпространение както и от други незаконни форми на обработване. Предприеманите мерки са съобразени със съвременните технологични постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени. При възникване и установяване на инцидент незабавно се докладва на лицето, отговорно за защита на личните данни и на администратора.

Чл. 48. Прилага се адекватна защита на личните данни, съобразена с нивото на нейното въздействие.

1. Физическа защита;
2. Персонална защита;
3. Документална защита;
4. Защита на автоматизирани информационни системи

Чл. 49. Физическа защита в Училището се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се обработват и съхраняват лични данни.

(1) Основните приложими организационни мерки за физическа защита в Училището включват определяне на помещенията, в които ще се обработват лични данни, както и на тези, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни, вкл. и определяне на организацията на физическия достъп.

Като помещения, в които ще се обработват лични данни, се определят всички помещения, в които с оглед нормалното протичане на учебния и административния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен само за служители с оглед изпълнение на служебните им задължения. Когато в тези помещения имат достъп и на външни лица, в помещенията се обособява непублична част, която е физически ограничена и достъпна само за служители, на които е необходимо да имат достъп, с оглед изпълнението на служебните им задължения.

Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в помещения, достъпът до които е ограничен само до тези служители, които за изпълнение на служебните си задължения се нуждаят от такъв достъп до данните, както и лицата, натоварени със служебни ангажименти за поддръжката на нормалното функциониране на тези системи. Последните нямат достъп до съхраняваните в електронен вид данни.

Организацията на физическия достъп до помещения, в които се обработват лични данни, е базирана на ограничен физически достъп (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения.

Като зони с контролиран достъп се определят всички помещения на територията на училището, в които се събират, обработват и съхраняват лични данни.

Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, са защитени по адекватен начин, в зони с контрол на достъпа.

(2) Основните приложими технически мерки за физическа защита в Училището включват използване на едно от следните: ключалки, шкафове, метални каси.

Чл. 50. Персоналната защита представлява система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора.

(1) Основните мерки на персоналната защита са:

1. познаване на нормативната уредба в областта на защитата на личните данни;
2. познаване на Политиката и ръководствата за защита на личните данни;
3. знания за опасностите за личните данни, обработвани от администратора;
4. споделяне на критична информация между персонала (например идентификатори,

5. пароли за достъп и т.н.);
 6. съгласие за поемане на задължение за неразпространение на личните данни;
- (2) Мерките за персонална защита гарантират достъпа до лични данни само на лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае“.
- (3) Лицата могат да започнат да обработват лични данни след запознаване със:
1. нормативната уредба в областта на защитата на личните данни;
 2. политиката и ръководствата за защита на личните данни;
 3. опасностите за личните данни, обработвани от администратора.

Чл. 51. Основните приложими мерки за документална защита на личните данни са:

1. Определяне на регистрите, които ще се поддържат на хартиен носител: на хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изисквания на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на училището;
2. Определяне на условията за обработване на лични данни: личните данни се събират само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната дейност на училището, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка;
3. Регламентиране на достъпа до регистрите: достъпът до регистрите е ограничен и се предоставя само на упълномощените служители, в съответствие с принципа на „Необходимост да знае“;
4. Определяне на срокове за съхранение: личните данни се съхраняват толкова дълго, колкото е необходимо, за да се осъществи целта, за която са били събрани и/или изискванията на действащото законодателство.
5. Процедури за унищожаване: Документите, съдържащи лични данни, които не подлежат на издаване към Държавен архив, и след изтичане на законовите срокове за тяхното съхранение и не са необходими за нормалното функциониране на Училището, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи).

Чл. 52. Защитата на автоматизирани информационни системи и/или мрежи в Училището включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

(1) Основните мерки за защита на автоматизирани информационни системи и/или мрежи, обработващи лични данни, оценени с ниско ниво на въздействие, включват:

1. Идентификация чрез използване на пароли за лицата, които имат достъп до мрежата и ресурсите на училището. Прилагането на тази мярка е с цел да се регламентират нива на достъп, съобразен с принципа „Необходимост да знае“;
2. Управление на регистрите, съобразено с ограничаване на достъпа до съответния регистър единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото въвеждане, поддръжка и обработка;
3. Защитата от вируси, включва използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира, инсталира и поддържа от учител по информационни технологии.
4. Политиката по създаване и поддържане на резервни копия за възстановяване регламентира - Основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на гимназията.
5. Основни електронни носители на информация са: вътрешни твърди дискове, еднократно и/или многократно презаписваеми външни носители (външни

твърди дискове, многократно презаписваеми карти, памети ленти и други носители на информация, еднократно записваеми носители и др.)

6. Персоналната защита на данните е част от цялостната охрана на гимназията.
7. Личните данни в електронен вид се съхраняват съгласно нормативно определените срокове и съобразно спецификата и нуждите на училището.
8. Данните, които вече не са необходими за целите на Училището и чийто срок за съхранение е изтекъл, се унищожават чрез приложим способ (напр. чрез нарязване, изгаряне или постоянно заличаване от електронните средства).

Чл. 53. Базисни правила и мерки за осигуряване на защита на личните данни при компютърна обработка

- (1) Компютърен достъп към файлове, съдържащи лични данни, се осъществява само от длъжностни лица с регламентирани права, единствено от тяхното физическо работно място, от специално определения за целта компютър и след идентификация чрез парола.
- (2) С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен период. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).
- (3) Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране на разумна степен на отказоустойчивост, възможности за архивиране и възстановяване на данните и работното състояние на средата.
- (4) При необходимост от ремонт на компютърната техника, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.
- (5) В училището се използва единствено софтуер с уредени авторски права.
- (6) На служебните компютри се използва само софтуер, който е инсталиран от оторизирано лице.
- (7) При внедряване на нов програмен продукт за обработване на лични данни се тестват и проверяват възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.
- (8) Служителите, на които е възложено да подписват служебна кореспонденция с универсален електронен подпис (УЕП), нямат право да предоставят издадения им УЕП на трети лица.

ОбУ „Неофит Рилски” прилага и следните допълнителни мерки:

1. Организация на телекомуникационните връзки и отдалечения достъп до вътрешните мрежи на институцията:

- ☐ Отдалечен достъп до вътрешни мрежи на институцията не се предвижда. По изключение, и след изричната оторизация от ръководството, може да се разреши подобен достъп от оторизираните лица, като за целта се използват адекватни и приложими съвременни методи за защита на връзката и обменните данни;
- ☐ На персонала на институцията може да бъде предоставен интернет достъп (отдалечен достъп) за изпълнение на служебните им задължения до електронните регистри с лични данни. Обхватът на достъпа и типа достъпни ресурси (вкл. сайтове, файлове, услуги и др.) се определя по преценка и предложение на преките ръководители, съгласувано с оторизираните от ръководството на институцията лица за степента на осъществимост, в пряка връзка с изпълняваните задължения и свързаните с този достъп рискове и одобрено от ръководството и след становище на ДЛЗД.
- ☐ Отдалеченият достъп чрез интернет до определени ресурси, вкл. и вътрешните такива, може да бъде прекратен по всяко време по преценка на ръководството, както и в случаите на заплахата за сигурността на данните.

2. Публикуването на служебна информация в интернет пространството, независимо под каква форма и на каква платформа, се извършва единствено след писмена оторизация от ръководството на институцията или от нарочно упълномощен за това служител.

(2) Мерките, свързани с текущото поддържане и експлоатация на информационните системи и ресурси на ОБУ „Неофит Рилски” включват:

□ Оценка на сигурността, включваща периодични тестове и оценки на уязвимостта на мрежите и системите на институцията от външни и вътрешни атаки, включително оценка на въздействието, адекватността на използваните мерки и способности за защита, както и препоръки за нейното техническо и организационно подобряване. Оценката включва посочените аспекти и по отношение сигурността на събираните, обработвани и съхранявани лични данни.

□ Забрана за притежание и ползване на хардуерни или софтуерни инструменти от персонала на институцията, ако същите биха могли да бъдат използвани, за да се компрометира сигурността на информационните системи. Към тази група се отнасят и инструменти, способстващи за нарушаване на авторските права, разкриване на тайни пароли, идентифициране на уязвимост в сигурността или дешифриране на криптирани файлове.

□ Забрана за използване на хардуер или софтуер, който отдалечено наблюдава трафика в мрежа или опериращ компютър. За неоторизирано използване на подобни инструменти служителят се наказва дисциплинарно, а ако то представлява престъпление – и по предвидения за санкциониране на това деяние ред.

(3) Мерките, свързани със създаване на физическа среда (обкръжение), включват физически контрол на достъпа (сигнално-охранителна техника, ключалки, метални решетки и други приложими способности), създаване на подходяща работна среда, вкл. чрез поддържане на подходяща температура и нива на влажност, както и пожароизвестителна система. Те са насочени към осигуряване на среда за нормално функциониране, за защита на ИТ оборудването от неоторизиран достъп и контрол на риска от повреда и унищожаване.

ХІІІ. ПОДДЪРЖАНИ РЕГИСТРИ С ЛИЧНИ ДАННИ И ТЯХНОТО УПРАВЛЕНИЕ

Чл. 54. Събирането, обработването и съхраняването на лични данни в регистрите на ОБУ „Неофит Рилски” се извършва на хартиен, технически и/или електронен носител по централизиран и/или разпределен способ в помещения, съобразно с предвидените мерки за защита и оценката на подходящото ниво на сигурност на съответния регистър.

(1) Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения.

(2) При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването ѝ, Училището може да определи друго ниво на защита за регистрите.

(3) Училището предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. защита при аварии, независещи от Училището – предприемат се конкретни действия в зависимост от конкретната ситуация;
2. защита от пожари - незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;
3. защита от наводнения- предприемат действия по ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.
- (4) Длъжностните лица - обработващи лични данни и оператори на лични данни предприемат всички организационно-технически мерки за съхраняването и опазването на личните данни.

(5) Отговарящите за отделните организационни и оперативни дейности, които формират целите на обработваната информация, осигурят създаването и поддържането на актуалността на информацията в регистрите. Всяка година те извършват преглед на актуалността.

ДЗЛД гарантира, че притежателите на информационни активи получават подходяща помощ за поддържане на регистъра.

(6) Поддържаните от ОБУ „Неофит Рилски” регистри с лични данни са:

- Ученици
- Персонал
- Родители
- Архив
- Доставчици
- Видеонаблюдение
- Пропускателен режим

Чл. 55. В регистър „Ученици“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица „ученици“, обучавани в Училището.

(1) Общо описание на регистър „Ученици“

Регистърът съдържа следните категории лични данни:

1. физическата идентичност на лицето: име, ЕГН, адрес, данни от ученическа карта, месторождение, телефони за връзка, акт за раждане;

2. лични данни, които се отнасят до здравето: ТЕЛК;

Нормативното основание е Законът за предучилищно и училищно образование, ЗПОО, КСО и приложимото законодателство, свързано с предоставянето на образователни услуги.

(2) Технологично описание на регистър „Ученици“:

- На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки. Папките се подреждат в шкафове в помещения на операторите на лични данни.

Информацията от хартиените носители за всеки ученик, се записва в подрегистрите както следва:

1.1. Книга за подлежащите на задължително обучение деца до 16-годишна възраст: предназначена за водене на отчет на деца от задължителната училищна възраст и се попълва с данни събрани за учениците от класните им ръководители и съдържа имена и ЕГН.

Данните от регистъра се предоставят доброволно от лицата при записването им.

1.2. Дневници: предназначени за вписване на информация за резултатите от учебната дейност на всеки ученик в една паралелка за една учебна година и съдържа имена, ЕГН и оценки. Води се от класния ръководител и всеки учител, който преподава в класа и се контролира от главния учител. Данните се събират за лицата в процес на обучението им в учебното заведение. Дневниците се съхраняват в учителската стая.

1.3. Книга за резултатите от изпитите на учениците от самостоятелна или индивидуална форма на обучение: Ползва се за вписване на резултатите от изпитите на учениците на самостоятелна и индивидуална форма на обучение. Книгата съдържа информация за: форма на обучение; учебна година; трите имена на ученика; ЕГН; месторождение; номер и дата на представените документи за образование; адрес по местоживее и телефон; резултати от изпитите по предмети, редове за вписване решение на педагогическия съвет – протокол номер, дата за завършване на годината; издаден документ, вид, номер, дата; определение състоянието на ученика – завършва, повтаря, ще полага изпит по предмет; име, фамилия и подпис на директора; печат. Книгата се води от директора или от длъжностно лице, определено със заповед на директора.

1.4. Регистрационна книга за издадените дубликати на документи за завършена степен на образование: предназначена за регистриране дубликати на свидетелства за основно образование, удостоверение за завършен гимназиален етап, дипломи за завършена

образователна степен. Съдържа информация за: регистрационен номер по реда на издаване на дубликата; регистрационен документ по ред за годината на издаване на дубликата; дата на регистриране на дубликата; трите имена на притежателя на дубликата; ЕГН, ЛНЧ; вид на издавания дубликат; серия; номер на бланката на дубликата; вид подготовка (непрофилирана, профилирана, специалност, професия); форма на обучение; серия, номер на бланката на оригинала на документа; регистрационния номер на оригиналния издаден документ; дата на издаване на оригинала; подпис на лицето при получаване на дубликата. Книгата се води от директора или от длъжностно лице, определено със заповед на директора.

1.5. Регистрационна книга за издадените документи и удостоверения: предназначена за регистриране на оригинали на: удостоверения за завършен първи клас; удостоверения за завършен начален етап на основно образование – IV клас; удостоверение за завършен клас. Регистърът съдържа информация за: пореден регистрационен номер; регистрационен номер за годината; дата на издаване; собствено, бащино и фамилно име на ученика; ЕГН; клас-група, чието завършване удостоверява документа; форма на обучение; подпис на получателя (родител-настойник). Книгата се води от директора или от длъжностно лице, определено със заповед на директора.

1.6. Копия на характеристики на ученика за завършена степен на образование: характеристика на ученика за завършена степен на образование се изготвя от класния ръководител за всеки ученик при придобиване на основно и на средно образование. Характеристика на ученика за завършена степен на образование съдържа следните реквизити: вид, наименование и местонахождение (град/село, община, област) на училището, издало характеристиката на ученика за завършена степен на образование; данни за притежателя на документа: собствено, бащино и фамилно име на ученика; ЕГН; дата и място на раждане; ЛНЧ; гражданство; форма на обучение; текст: „е завършил/а основно/средно образование през учебнатагод“; описание на цялостното развитие на ученика през съответната степен на образование; дата на издаване; име, фамилия и подпис на класния ръководител.

1.7. Инструктажна книга за безопасни условия на обучение, възпитание и труд.

1.8. Главна книга: Главната книга служи за вписване на годишните оценки на всички ученици от I до IV. Книгата се води от учител, определен със заповед на училищния ръководител или от училищния ръководител. Книгата се попълва въз основа данните на учениците, съдържащи се в дневниците на класовете за съответната учебна година.

- На технически носител: Личните данни се въвеждат в специализирана Информационна система за училищна администрация Админ Про. Базата данни се намира на твърдия диск на изолирани компютри.

Срок на съхранение: съгласно Номенклатурата на делата в ОБУ „Неофит Рилски“ със срокове на съхранение;

(3) Определяне на длъжностите:

Обработващи лични данни на регистър „Ученици“ са: директор, ЗАС, главен счетоводител и класни ръководители.

Оператор на лични данни на регистър „Ученици“ е целия педагогически персонал.

(4) Достъп до регистър „Ученици“ имат и държавните органи – МОН, РУО, дирекция „Социално подпомагане“ за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове. Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

(5) Лични данни на учениците се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Номенклатурата на делата със сроковете за тяхното съхранение в Училището.

Чл. 56. В регистър „Персонал“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, назначени по трудово правоотношение и/или и по граждански договори.

(1) Общо описание на регистър „Персонал“

Регистърът съдържа следните групи данни:

1. физическата идентичност - име, ЕГН, адрес, паспортни данни, месторождение, телефони за връзка и банкови сметки;
2. социална идентичност - образование и трудова дейност;
3. лични данни, които се отнасят до здравето – медицинско свидетелство;
4. други - лични данни относно гражданско-правния статус на лицата – свидетелство за съдимост;

Нормативното основание е Кодексът на труда, Кодексът за социалното осигуряване, Законът за счетоводството, Законът за данъците върху доходите на физическите лица и приложимото законодателство в областта на трудовото право.

Предназначението на събираните данни в регистъра е свързано с :

1. Индивидуализиране на трудовите правоотношения;
2. Изпълнение на нормативните изисквания на свързаното с регистъра приложимо действащо законодателство;
3. Дейностите, свързани със сключване, съществуване, изменение и прекратяване на трудовите правоотношения, изготвяне на договори, допълнителни споразумения, заповеди, документи, удостоверяващи трудовия стаж, доходите от трудови правоотношения и по граждански договори, служебни бележки, справки, удостоверения и др.
4. Установяване на връзка с лицето по телефон, изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудово правоотношение и по граждански договори.

(2) Технологично описание на регистър „Персонал“:

2.1. На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки (трудова досиета), ако е изискуемо.

2.2. На технически носител: Личните данни се въвеждат в специализирана Информационна система за училищна администрация Админ Про. Базата данни се намира на твърдия диск на изолирани компютри.

Срок на съхранение: съгласно Номенклатурата на делата в ОБУ „Неофит Рилски“ със срокове на съхранение;

(3) Определяне на длъжностите:

Обработващи лични данни на регистър „Персонал“ са: директор, гл.счетоводител и ЗАС. Оператор на лични данни на регистър „Персонал“ е директорът.

(4) Достъп до регистър „Персонал“ имат и държавните органи – НАП, НОИ, МОН, РУО за изпълнение на техните задължения, предвидени в съответните закони и подзаконови нормативни актове. Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

(5) Лични данни се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Номенклатурата на делата със сроковете за тяхното съхранение в Училището.

Чл.57. В регистър Архив се съхраняват лични данни:

- на работилите в учебното заведение по трудови правоотношения; на физическите лица, сключили договори със заведението на различни основания, както и на други лица, предоставили доброволно личните си данни;
- на учащите се и учителите в учебното заведение;

- родителите/ настойниците на учащите
- 1. Съхраняване на предоставените документи в предвидените срокове;
- 2. Изпълнение на нормативните изисквания на Кодекса на труда, Закона за народната просвета, Правилника за прилагане на закона за народната просвета, Наредба 4/2003г. за документите за системата на народната просвета. Закона за задълженията и договорите, Закона за държавния архив, Номенклатурата за водене и съхранение на делата, Инструкция за документооборота и др.;
- 3. Използване на събраните данни за служебни цели, свързани с изготвяне на справки, издаване на документи и други статистически и исторически цели. Данните се съхраняват в писмена (документална) форма и се класират в архивни дела, съответстващи на въведената инструкция за архивиране /деловодна обработка/. Делата не се изнасят извън сградата на администратора.
- (1) Формата на водене на регистъра е на хартиен носител:
 1. Данните се съхраняват в писмена (документална) форма и се класират в архивни дела, съответстващи на въведената инструкция за архивиране /деловодна обработка/
 2. Делата се подреждат в специални шкафове, които са разположени в изолирано помещение със защитна сигнализация.
 3. Длъжностните лица предприемат всички организационни мерки за съхраняването и опазването на делата, в това число изолиране на достъпа до тях на външни лица и служители.
 4. Делата не се изнасят извън сградата на администратора.
- (2) В регистър Архив се съхраняват следните групи лични данни:
 1. Относно физическата идентичност на лицата: имена, ЕГН, адрес по местоживее и др.;
 2. Относно образованието: степен на образованието, придобита специалност, допълнителна квалификация и др.;
 3. Относно трудовата дейност: професионална биография, трудов стаж и др.;
 4. Относно здравния статус на лицата;
 5. Относно гражданско-правния статус на лицата: свидетелство за съдимост;
 6. Относно икономическата идентичност: финансово състояние и др.;
- (3) Право на достъп до данните в регистъра имат: лицата за които се отнасят данните в регистъра, по тяхно изрично искане; Директора, Главния счетоводител, учителите и ЗАС при изпълнение на правомощията им по Кодекса на труда и длъжностна характеристика; Държавни органи надлежно легитимирани се със съответни документи.
- (4) Срок на съхранение: съгласно Номенклатурата на делата в ОБУ „Неофит Рилски” със срокове на съхранение

Чл. 58. В регистър „Родители“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, родители, настойници и други категории, свързани с тях лица.

(1) Общо описание на регистър „Родители“

Регистърът съдържа следните групи данни:

1. физическата идентичност - име, ЕГН, адрес/ местожителство, телефони за връзка; Нормативното основание е Законът за предучилищно и училищно образование и приложимото законодателство, свързано с предоставянето на образователни услуги.

(2) Технологично описание на регистър „Родители“:

2.1. На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки, ако е изискуемо.

2.2. На технически носител: Личните данни се въвеждат в специализирана Информационна система за училищна администрация Админ Про. Базата данни се намира на твърдия диск на изолирани компютри.

Срок на съхранение: съгласно Номенклатурата на делата в Училището със срокове на съхранение;

(3) Определяне на длъжностите:

Обработващи лични данни на регистър „Родители“ са: директор, гл. счетоводител, ЗАС и класни ръководители.

Оператор на лични данни на регистър „Родители“ е целия педагогически персонал.

(4) Достъп до регистър „Родители“ имат и държавните органи – МОН, РУО, дирекция „Социално подпомагане“ за изпълнение на техните задължения, предвидени в съответните закони и подзаконови нормативни актове. Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

(5) Лични данни се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Номенклатурата на делата със сроковете за тяхното съхранение в Училището.

Чл. 58а. В регистър „Доставчици“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за счетоводството. Категориите физически лица, за които се обработват лични данни, са доставчици, с които работи Училището.

(1) Общо описание на регистър „Доставчици“

Регистърът съдържа следните групи данни - физическата идентичност: наименование, булстат, седалище, име и телефон за връзка на представител и банкова сметка.

(2) Технологично описание на регистър „Доставчици“: Данните се набират в писмена форма в първични счетоводни документи.

(3) Определяне на длъжностите:

Обработващ лични данни на регистър „Доставчици“ е главен счетоводител.

Оператор на лични данни на регистър „Доставчици“ е директорът.

(4) Достъп до регистър „Доставчици“: Категориите лица, на които личните данни могат да бъдат разкривани са физически лица, за които се отнасят данните, и на лица, ако е предвидено в нормативен акт, на лица по силата на договор.

(5) Лични данни се съхраняват до осъществяване на целите, за които се обработват.

(6) Източниците, от които се събират данните, са: от юридически лица и техни представители - физически лица.

(7) Данните в регистъра се предоставят доброволно при съставяне на счетоводните документи.

Чл. 59. В регистър „Видеонаблюдение“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност. Цялата информация за регистър „Видеонаблюдение“ може да намерите във „Вътрешната Политика за защита на личните данни, създадени чрез видеонаблюдение“ на Училището.

Чл. 60. В регистър „Пропускателен режим“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност. Категориите физически лица, за които се обработват лични данни, са посетителите в сградата на училището.

(1) Общо описание на регистър „Пропускателен режим“

Регистърът съдържа следните групи данни - физическата идентичност: имена на лицето по лична карта.

(2) Технологично описание на регистър „Пропускателен режим“: Данните се набират в писмена форма в дневник.

(3) Определяне на длъжностите:

Обработващ лични данни на регистър „Пропускателен режим“ е охраната.

Оператор на лични данни на регистър „Пропускателен режим“ е главен учител.

(4) Източниците, от които се събират данните, са: от физическите лица.

Лични данни се съхраняват до осъществяване на целите, за които се обработват (до приключване на дневника). След приключване на дневника, същият се унищожава физически.

(5) Данните в регистъра се предоставят доброволно от лицата при влизането им в сградата на училището.

XIV. СЪХРАНЯВАНЕ И УНИЩОЖАВАНЕ НА ЛИЧНИТЕ ДАННИ

Съхраняване на лични данни

- Чл.61. (1) Документите и регистрите, по които работата е приключила, се архивират.
- (2) Трайното съхраняване за нуждите на архивирането на документи на хартиен носител, съдържащи лични данни, се извършва в помещения, определени за архив, за срокове, съобразени с действащото законодателство и тези Правила. Помещенията, определени за архив, са оборудвани с пожароизвестителни системи и пожарогасители, със системи за контрол на достъпа и задължително се заключват.
- (3) Документите на електронен носител се съхраняват на специализирани сървъри, компютърни системи и/или външни носители на информация.
- (4) Архивиране на личните данни на технически носител се извършва периодично (всеки ден, всяка седмица или всеки месец – в зависимост от указанията на системния администратор и ДЛЗД за всеки носител и категория данни) от опериращия с личните данни служител с оглед запазване на информацията за съответните лица в актуален вид и с цел осигуряване на възможност за възстановяване, в случай на погиване на основния носител/система. Архивните копия се съхраняват на местоположение, различно от мястото на компютърното оборудване, с което се обработват данните.
- (5) Архивирането по предходната алинея се извършва на надеждни оптични носители (сървъри, външни твърди дискове, USB-флашки и др.), достъп до които има само обработващият съответните лични данни и изрично оторизирани за това длъжностни лица.

- Чл.62. (1) С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.
- (2) Служителите преминават задължителен инструктаж за запознаване с правилата за противопожарна безопасност най-малко веднъж годишно. За проведения инструктаж се съставя Протокол по образец.

- Чл.63. (1) Най-малко веднъж годишно се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в обработваните от институцията регистри.
- (2) Резултатите от всяка проверка се обобщават в доклад на ДЛЗД до директора на институцията, в който се включва и преценка на необходимостта за обработка на личните данни или тяхното унищожаване.

Срокове на съхраняване на лични данни

- Чл.64. (1) ОБУ „Неофит Рилски” не съхранява лични данни във вид, който позволява идентифицирането на субектите за по-дълъг период отколкото е необходимо, по отношение на целите, за които са били събрани данните или за срок, установен като изискуем съгласно нормативната уредба.
- (2) Образователната институция може да съхранява данни за по-дълги периоди единствено ако личните данни ще бъдат обработвани за целите на архивиране, за цели в обществен интерес, научни или исторически изследвания и за статистически цели, и само при изпълнението на подходящи технически и организационни мерки за гарантиране на правата и свободите на субекта на данните.

Унищожаване на лични данни

Чл.65.(1) След постигане целта на обработване на личните данни, съдържащи се в поддържаните от ОБУ „Неофит Рилски” регистри, личните данни следва да бъдат унищожени при спазване на процедурите, предвидени в приложимите нормативни актове и в настоящите Вътрешни правила.

(2) В случаите, в които се налага унищожаване на носител на лични данни, ОБУ „Неофит Рилски” прилага необходимите действия за заличаването на личните данни по начин, изключващ възстановяване данните и злоупотреба с тях, като:

1. Личните данни, съхранявани на електронен носител и сървъри, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите;

2. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване с шредер машина.

(3) Личните данни трябва да бъдат унищожени сигурно, съгласно принципа за гарантиране подходящо ниво на сигурност (чл. 5, пар.1, б.„е” от ОРЗД).

(4) При унищожаване на личните данни не трябва да бъдат накърнявани правата на лицата, за които се отнасят данните, обект на унищожаването.

Чл.66. (1) Унищожаването се осъществява от служители, упълномощени с изричен писмен акт на директора и след задължително уведомяване на Длъжностното лице по защита на данните.

(2) За извършеното унищожаване на лични данни и носители на лични данни се съставя Протокол, подписан от служителите по предходната алинея.

XV. ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

Достъп, предоставян на компетентните държавни / общински органи

Чл.67. Достъпът на трети лица до лични данни обработвани от ОБУ „Неофит Рилски” е категорично забранен, освен предвидените в закона и/или в настоящите Вътрешни правила случаи.

Чл.68. (1) ОБУ „Неофит Рилски” осигурява достъп до обработваните лични данни на физически лица, когато същите са изискани по надлежен ред от компетентни държавни и/или общински органи (МОН, РУО на МОН, НАП, НОИ и др.) и когато задължението за предоставяне на данните е предвидено в нормативен акт.

(2) На компетентните органи се осигурява достъп до личните данни или данните се предоставят съгласно законовите изисквания в зависимост от всеки конкретен случай.

(3) Решението си за предоставяне или отказ на достъп до лични данни за съответното лице инситуцията съобщава на третите лица в подходящ срок от подаване искането, без ненужно забавяне.

Предоставяне на данни на обработващ

Чл.69. (1) ОБУ „Неофит Рилски” може, при необходимост и във връзка с дейността си, да предоставя лични данни на трети лица, действащи в качеството на обработващ.

(2) Инситуцията избира за обработващ(и) само доставчици, които могат да осигурят и гарантират техническа, физическа и организационна сигурност и които отговарят на поставените изисквания по отношение на всички лични данни, които ще обработват

(3) Взаимоотношенията с обработващ(и) задължително се регламентират с изричен писмен акт.

(4) При сключването на договор/споразумение с обработващ, ОБУ „Неофит Рилски” задължително:

1. предвижда и изисква от обработващия достатъчно гаранции за спазване на законовите изисквания и добрите практики за обработка и защита на личните данни;

2. информира за предоставянето физическите лица, чиито данни ще бъдат предадени на обработващ.

Трансфер на данни извън ЕС

Чл.70. (1) ОБУ „Неофит Рилски” не извършва трансфер и не предоставя лични данни в страни извън ЕС.

(2) При възникнала необходимост, такъв трансфер, може да се реализира само при някоя от следните хипотези:

1. субектът на данните изрично се е съгласил с предложеното прехвърляне, след като е бил информиран за възможните рискове от такива прехвърляния;
 2. предаването е необходимо за изпълнението на договор между субекта на данните и администратора или за изпълнението на преддоговорни мерки, взети по искане на субекта на данните;
 3. предаването е необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данните между администратора и друго физическо или юридическо лице;
 4. предаването е необходимо поради важни причини от обществен интерес;
 5. предаването е необходимо за установяването, упражняването или защитата на правни претенции;
 6. предаването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на други лица, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;
 7. предаването се извършва от регистър, който съгласно правото на ЕС или правото на държавите членки е предназначен да предоставя информация на обществеността и е достъпен за справка от обществеността по принцип или от всяко лице, което може да докаже, че има законен интерес за това, но само доколкото условията за справка, установени в правото на Съюза или правото на държавите членки, са изпълнени в конкретния случай.
- (3) За предоставянето на данните се сключва писмено споразумение (договор).

XVI. ДЕЙСТВИЯ ПРИ НАРУШЕНИЯ НА СИГУРНОСТТА

Общи положения

Чл.71. (1) Нарушение на сигурността на личните данни е всяко събитие, при което се реализира случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или неоторизиран достъп до лични данни, които се предават, съхраняват или обработват по друг начин.

(2) Нарушение на сигурността на личните данни е и всяко действие или бездействие, което компрометира сигурността, конфиденциалността или целостта на данните, или на физическите, технически, административни или организационни защити.

(3) Не е нарушение на сигурността констатираният потенциален риск от възникване на събитие по ал.1, без същото да се е реализирало.

Процедурни действия при установяване на нарушение

Чл.72.(1) При всяко идентифициране на признаци за нарушение на сигурността, лицето което го е констатирало е длъжно да докладва на ДЛЗД, а когато това е невъзможно, на директора на институцията.

(2) Докладването се извършва в писмена форма, по имейл или друг подходящ начин, който позволява да се установи извършването и документирането на нарушението, да се определи и спази срока за уведомяване. При докладването служителят предоставя цялата налична информация по случая и предприема необходимите действия и мерки за съхраняване на всички доказателства свързани с нарушението.

(3) ДЛЗД извършва незабавна проверка на подадения по ал.1 сигнал, като при проверката установява реализирано ли е нарушение на сигурността, в какво се изразява нарушението, кои данни са засегнати и до кои субекти на данни се отнасят.

(4) При спешност и когато това е възможно и допустимо, ДЛЗД предприема мерки за преустановяване на нарушението, неутрализиране или редуциране на щетите от него.

(5) ДЛЗД докладва незабавно на директора на институцията за нарушението на сигурността на данните, като предоставя информация за вида на нарушението, времето на установяване,

XVII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Настоящите правила са в сила и се прилагат от 25.05.2018 г.

§ 2. (1) За всички неуредени в настоящите Вътрешни правила въпроси, са приложими разпоредбите на Общия регламент относно защитата на данните (ЕС) 2016/679, приложимото право на Европейския съюз и законодателството на Република България относно защитата на личните данни.

(2) Разработените към настоящите Вътрешни правила приложения са примерни образци на документи, които се съставят при и по повод обработката на лични данни:

§ 3. (1) Изменения и допълнения на Вътрешните правила се правят по реда на издаването и утвърждаването им.

(2) ОБУ „Неофит Рилски” може да променя тези Правила по всяко време.

(3) Всички промени незабавно се свеждат до знанието на лицата, които засягат.

§ 4. Всички лица с ръководни функции в ОБУ „Неофит Рилски” носят отговорност за спазването на тези правила от страна на персонала и следва да въведат подходящи практики, процеси и обучение.

§ 5. (1) Настоящите Вътрешни правила се свеждат до знанието на всички служители на образователната институция, както и до ангажираните с изпълнение на граждански договор лица.

(2) Лицата по ал.1 са длъжни да спазват Правилата ежедневно при изпълняване на заемната от тях длъжност и възложената им работа.

(3) За неизпълнение на задълженията по Правилата и действащото към съответния момент национално и европейско законодателство за защита на личните данни, съответните лица носят дисциплинарна и имуществена отговорност.

§ 6. Контрол по изпълнението на настоящите Вътрешни правила за обработване и защита на лични данни се осъществява от Директора и Длъжностното лице по защита на данните.

Последна актуализация 20.09.2023 г.

ПРИЛОЖЕНИЯ

№	Наименование на приложението
1.	Приложение 1: Регистър на дейности по обработване на лични данни (администратор) 1.1. Регистър на категории дейности по обработването (обобщаващ)
2.	Приложение 2 Регистър на лицата, обработващи лични данни 2.1. Списък на лица, които обработват лични данни
3	Приложение 3: Декларация за поверителност на данните

ДОПЪЛНЕНИЕ № 1

Оценка на нивото на въздействие на регистър

	НИВО НА ВЪЗДЕЙСТВИЕ			
	поверителност	цялостност	наличност	общо за регистъра
Име на регистъра				
Персонал	високо	високо	високо	високо
Ученици	високо	високо	високо	високо
Родители и настойници	високо	високо	високо	високо
Доставчици	ниско	ниско	ниско	ниско
Видеонаблюдение	високо	високо	високо	високо
Архив	високо	високо	високо	високо
Пропускателен режим	високо	високо	високо	високо

ДОПЪЛНЕНИЕ № 2

ПРОТОКОЛ за преминат инструктаж по защита на личните данни за приложимата в ОБУ „Неофит Рилски” Вътрешна политика за защита на лични данни при видеонаблюдение и Вътрешна политика за мерките за защита на личните данни съгласно Регламент 2016/679.

- Бланката се попълва от целия персонал/ служители на ОБУ „Неофит Рилски”, посредством вписване на име, фамилия и подпис.

